Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
_____ В. В. Павліков
(підпис) (ініціали та прізвище)
«__» 08 2020 р.
Відділ аспірантури і докторантури

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Методи пентестінгу та кіберзахисту розподілених систем
(назва навчальної дисципліни)

Галузь знань: 12 "Інформаційні технології"
(шифр і найменування галузі знань)

Спеціальність: 125 "Кібербезпека"
(код та найменування спеціальності)

Освітньо-наукова програма: "Кібербезпека"
(назва освітньої програми)

Форма навчання: денна

Рівень вищої освіти: третій (освітньо-науковий)

Харків 2020 рік

РОБОЧА ПРОГРАМА
ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Методи пентестінгу та кіберзахисту розподілених систем
(назва дисципліни)

для здобувачів за спеціальністю 125 "Кібербезпека"

освітньо-наукової програми "Кібербезпека"

«26» 08 2020 р., – 12 с.

Розробник: асистент (підпис) Тецький А. Г.
(посада, науковий ступінь та вчене звання) (прізвище та ініціали)

Розробник: доцент, к.т.н., доцент (підпис) Узун Д. Д.
(посада, науковий ступінь та вчене звання) (прізвище та ініціали)

Гарант ОНП доцент, к.т.н. (підпис) Колісник М.О.
(посада, науковий ступінь та вчене звання) (прізвище та ініціали)

Протокол №1 від «27» серпня 2020 р. засідання кафедри № 503

Завідувач кафедри д.т.н., професор (підпис) Харченко В. С.
(науковий ступінь та вчене звання) (прізвище та ініціали)

ПОГОДЖЕНО:

Завідувач відділу
аспірантури і докторантури В. Б. Селевко

Голова наукового товариства
студентів, аспірантів,
докторантів і молодих вчених Т. П. Старовойт

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітня програма, рівень вищої освіти	Характеристика навчальної дисципліни
		Денна форма навчання
Кількість кредитів – 5	**Галузь знань** 12 "Інформаційні технології" (шифр та найменування)	Вибіркова
Кількість модулів – 1		**Навчальний рік**
Кількість змістовних модулів – 2	**Спеціальність** 125 "Кібербезпека" (код та найменування)	2020/ 2021
Індивідуальне завдання немає		**Семестр**
Загальна кількість годин – 68 / 150	**Освітньо-наукова програма** «Кібербезпека» (найменування)	4-й
		Лекції [1)]
		34 години
Кількість тижневих годин для денної форми навчання: аудиторних – 4 самостійної роботи аспіранта – 4,8	**Рівень вищої освіти:** третій (освітньо-науковий)	**Практичні, семінарські** [1)]
		0 годин
		Лабораторні [1)]
		34 години
		Самостійна робота
		82 години
		Вид контролю
		іспит

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: для денної форми навчання – 68 / 82.

[1)] Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета: дати знання про сучасні методи наукового дослідження пентестінгу та кіберзахисту розподілених інформаційних систем для забезпечення і дослідження гарантоздатної обробки, передачі та зберігання інформації.

Завдання: вивчення і дослідження основних методів пентестінгу, методів і моделей кіберзахисту інформації в гарантоздатних розподілених інформаційних системах.

Згідно з вимогами освітньо-професійної програми аспіранти повинні досягти таких **компетентностей:**

- здатність до абстрактного мислення, аналізу та синтезу;
- здатність до пошуку, оброблення та аналізу інформації з різних джерел;
- здатність застосовувати сучасні інформаційні технології, бази даних та інші електронні ресурси, спеціалізоване програмне забезпечення у науковій та навчальній діяльності;
- здатність до продукування нових ідей і розв'язання комплексних проблем у галузі інформаційних технологій, а також до застосування сучасних методологій, методів та інструментів педагогічної та наукової діяльності в кібербезпеці.

Програмні результати навчання:

- застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи;
- знати, розуміти та вміти застосовувати методи та засоби створення інформаційних технологій та програмного забезпечення розподілених систем, Інтернету речей, хмарних обчислень, систем штучного інтелекту, віртуальної реальності у предметних областях різних галузей, в тому числі в аерокосмічній галузі.

Міждисциплінарні зв'язки. Дисципліна є вибірковою компонентою освітньо-наукової програми «Кібербезпека» і базується на знаннях, отриманих під час вивчення дисциплін «ІТ в практиці наукових досліджень», «Теорія і методи зеленої ІТ-інженерії», «Наукові англомовні комунікації», «Теорія і технології критичного комп'ютингу», «Теорія планування експерименту», що є обов'язковими компонентами.

Матеріал, засвоєний під час вивчення цієї дисципліни, є базою для підготовки дисертаційної роботи.

3. Програма навчальної дисципліни

Модуль 1.

Змістовний модуль 1. Огляд сучасних проблем кібербезпеки веб-застосунків.

Тема 1. Підготовка тестового оточення. Встановлення Damn Vulnerable Web Application.

Встановлення на локальній машині платформи з вразливостями для наукового дослідження. Закріплення навичок роботи в Linux-подібних системах. Отримання навичок встановлення і налаштування веб-сервера для подальшого встановлення на нього вразливого застосунка.

Тема 2. Аналіз трафіку комп'ютерних мереж і наукове дослідження сценарію атаки типу Man-in-the-Middle.

Отримання навичок роботи з аналізатором трафіку Wireshark і платформою Burpsuite, знайомство з атакою Man-in-the-Middle. Знайомство зі структурою мережевих пакетів. Отримання навичок роботи в сніффером на прикладі Wireshark і Burpsuite. Аналіз сценаріїв MitM-атак веб-застосунку. Розробка методів захисту веб-застосунку від даного виду атак.

Тема 3. SQL-ін'єкції. Принципи, пошук і експлуатація SQL-ін'єкцій. Методи ін'єкцій та їх наслідки.

Атаки з порушенням логіки запитів до бази даних. Робота з інструментальним засобом для пошуку і експлуатації ін'єкцій. Освоєння природи походження і принципів експлуатації вразливості в браузері. Отримання навичок використання утиліти sqlmap для експлуатації SQL-ін'єкцій. Порівняльний аналіз та наукове дослідження методів ін'єкцій при різній складності експлуатації вразливостей в DVWA.

Тема 4. Робота з XSS-атаками. Особливості атак та їх наслідки.

Сценарії здійснення атак та інструменти атак. Освоєння природи походження і принципів експлуатації вразливості в браузері. Отримання навичок використання утиліти xsser для пошуку вразливостей. Можливості XSS-атак. Розроблення заходів щодо захисту веб-застосунка від XSS-атак.

Змістовний модуль 2. Аналіз проблем кібербезпеки мереж та системного програмного забезпечення.

Тема 5. Робота з шеллом в Metasploit. Наукове дослідження можливостей виконання довільних команд в атакованій системі.

Отримання навичок роботи в фреймворку на прикладі модуля управління шеллом. Отримання навичок використання модулів фреймворка Metasploit. Отримання навичок управління атакованим сервером. Можливі наслідки експлуатації шелл. Розроблення заходів щодо захисту веб-застосунка від завантаження шелл.

Тема 6. Основи сканування IP-мереж.

Знайомство з призначенням і функціоналом утиліти nmap в ОС Kali Linux, знайомство з основними відкритими базами даних вразливостей. Отримання навичок використання утиліти nmap. Отримання навичок пошуку

інформації у відкритих базах вразливостей. Наукове дослідження методів і засобів виявлення сканування. Розроблення заходів щодо захисту мережі від сканування.

Тема 7. Забезпечення безпеки багатокомпонентного веб-застосунка.

Аналіз можливих проблем безпеки веб-застосунка на етапі проєктування. Список вимог, які повинні бути перевірені перед здачею проєкту замовнику. Методи і засоби захисту від поширених атак. Наукове дослідження методів Web Application Firewall для виявлення потенційно небезпечного трафіку.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовний модуль 1. Огляд сучасних проблем кібербезпеки веб-застосунків.					
Тема 1. Підготовка тестового оточення. Встановлення Damn Vulnerable Web Application.	18	4		4	10
Тема 2. Аналіз трафіку комп'ютерних мереж і наукове дослідження сценарію атаки типу Man-in-the-Middle.	20	4		4	12
Тема 3. SQL-ін'єкції. Принципи, пошук і експлуатація SQL-ін'єкцій. Методи ін'єкцій та їх наслідки.	20	4		4	12
Тема 4. Робота з XSS-атаками. Особливості атак та їх наслідки.	20	4		4	12
Модульний контроль	1			1	
Разом за змістовним модулем 1	**79**	**16**		**17**	**46**
Змістовний модуль 2. Аналіз проблем кібербезпеки мереж та системного програмного забезпечення.					
Тема 5. Робота з шеллом в Metasploit. Наукове дослідження можливостей виконання довільних команд в атакованій системі.	23	6		5	12

Тема 6. Основи сканування IP-мереж.	23	6		5	12
Тема 7. Забезпечення безпеки багатокомпонентного веб-застосунка.	24	6		6	12
Модульний контроль	1			1	
Разом за змістовним модулем 2	**71**	**18**		**17**	**36**
Усього годин	**150**	**34**		**34**	**82**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	*Не передбачено*	
	Разом	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	*Не передбачено*	
	Разом	

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Підготовка тестового оточення. Встановлення Damn Vulnerable Web Application. - Встановлення на локальній машині платформи з вразливостями для наукового дослідження. - Закріплення навичок роботи в Linux-подібних системах. - Отримання навичок встановлення і налаштування веб-сервера для подальшого встановлення на нього вразливого застосунка.	4

2	Аналіз трафіку комп'ютерних мереж і наукове дослідження сценарію атаки типу Man-in-the-Middle. - Отримання навичок роботи з аналізатором трафіку Wireshark і платформою Burpsuite, знайомство з атакою Man-in-the-Middle. - Знайомство зі структурою мережевих пакетів. - Отримання навичок роботи в сніффером на прикладі Wireshark і Burpsuite. - Аналіз сценаріїв MitM-атак веб-застосунку. - Розроблення методів захисту веб-застосунку від даного виду атак.	4
3	SQL-ін'єкції. Принципи, пошук і експлуатація SQL-ін'єкцій. Методи ін'єкцій та їх наслідки. - Атаки з порушенням логіки запитів до бази даних. - Робота з інструментальним засобом для пошуку і експлуатації ін'єкцій. - Освоєння природи походження і принципів експлуатації вразливості в браузері. - Отримання навичок використання утиліти sqlmap для експлуатації SQL-ін'єкцій. - Наукове дослідження методів ін'єкцій при різній складності експлуатації вразливостей в DVWA.	4
4	Робота з XSS-атаками. Особливості атак та їх наслідки. - Сценарії здійснення атак та інструменти атак. - Освоєння природи походження і принципів експлуатації вразливості в браузері. - Отримання навичок використання утиліти xsser для пошуку вразливостей. - Можливості XSS-атак. Розроблення заходів щодо захисту веб-застосунка від XSS-атак.	4
5	Робота з шеллом в Metasploit. Наукове дослідження можливостей виконання довільних команд в атакованій системі. - Отримання навичок роботи в фреймворку на прикладі модуля управління шеллом. - Отримання навичок використання модулів фреймворка Metasploit. - Отримання навичок управління атакованим сервером. - Можливі наслідки експлуатації шелл. - Розроблення заходів щодо захисту веб-застосунка від завантаження шелл.	5

6	Основи сканування IP-мереж. - Знайомство з призначенням і функціоналом утиліти nmap в ОС Kali Linux, знайомство з основними відкритими базами даних вразливостей. - Отримання навичок використання утиліти nmap. - Отримання навичок пошуку інформації у відкритих базах вразливостей. - Наукове дослідження методів і засобів виявлення сканування. Розроблення заходів щодо захисту мережі від сканування.	5
7	Забезпечення безпеки багатокомпонентного веб-застосунка. - Аналіз можливих проблем безпеки веб-застосунка на етапі проєктування. - Список вимог, які повинні бути перевірені перед здачею проєкту замовнику. - Методи і засоби захисту від поширених атак. - Наукове дослідження методів Web Application Firewall для виявлення потенційно небезпечного трафіку.	6
	Разом	32

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Підготовка тестового оточення. Встановлення Damn Vulnerable Web Application.	10
2	Аналіз трафіку комп'ютерних мереж і наукове дослідження сценарію атаки типу Man-in-the-Middle.	12
3	SQL-ін'єкції. Принципи, пошук і експлуатація SQL-ін'єкцій. Методи ін'єкцій та їх наслідки.	12
4	Робота з XSS-атаками. Особливості атак та їх наслідки.	12
5	Робота з шеллом в Metasploit. Наукове дослідження можливостей виконання довільних команд в атакованій системі.	12
6	Основи сканування IP-мереж.	12
7	Забезпечення безпеки багатокомпонентного веб-застосунка.	12
	Разом	**82**

9. Індивідуальні завдання

Не передбачено

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота аспірантів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

12. Критерії оцінювання та розподіл балів, які отримують аспіранти

12.1. Розподіл балів, які отримують аспіранти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0…0,5	8	0…4
Виконання і захист лабораторних робіт	0...6	4	0...24
Модульний контроль	0…25	1	0…25
Змістовний модуль 2			
Робота на лекціях	0…0,5	8	0…4
Виконання і захист лабораторних робіт	0...6	3	0...18
Модульний контроль	0…25	1	0…25
Усього за семестр			**0…100**

Семестровий контроль у вигляді іспиту проводиться у разі відмови аспіранта від балів поточного тестування. Під час складання семестрового іспиту аспірант має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних та одного практичного запитань, максимальна кількість балів за кожне із запитань складає 33 бали.

12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки

1. Знати особливості функціонування ОС Linux
2. Знати основні команди для роботи в ОС Linux
3. Знати принципи роботи серверного програмного забезпечення під керуванням ОС Linux

Необхідний обсяг умінь для одержання позитивної оцінки

1. Уміти працювати з файловою системою в ОС Linux
2. Уміти встановлювати програмне забезпечення в ОС Linux
3. Уміти розробляти скрипти на мові shell
4. Уміти працювати з інструментальними засобами пошуку проблем безпеки в ОС Linux

12.3 Критерії оцінювання роботи аспіранта протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 75% від усіх завдань лабораторних занять.

Добре (75-89). Твердо знати мінімум, захистити не менше 90% завдань лабораторних занять.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

Навчально-методичний комплекс дисципліни розміщений у системі управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки.

1. Система управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки [Ел. ресурс]. URL: https://moodle.csn.khai.edu

14. Рекомендована література

Базова

1. Ric Messier. Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems / Apress, 2016. – 115 p.
2. Ron Lepofsky. The Manager's Guide to Web Application Security: A Concise Guide to the Weaker Side of the Web / Apress, 2014. – 232 p.
3. David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni. Metasploit. – 2011. – 328 p.
4. А. Г. Тецький, О. О. Ілляшенко, Д. Д. Узун. Методи та засоби тестування на проникнення веб-додатків і мереж. Практикум / під ред. В.С. Харченка – Міністерство освіти і науки України, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ». 2017. – 77 с.

Допоміжна

1. William Shotts. The Linux Command Line, 2nd Edition: A Complete Introduction. – No Starch Press, 2019. – 504 p.

2. OccupyTheWeb. Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali. – No Starch Press, 2018. – 504 p.

15. Інформаційні ресурси

1. https://www.kali.org/
2. https://nvd.nist.gov/
3. https://owasp.org/
4. http://csn.khai.edu